Definitions and Concepts for OCR Computer Science A-level

Component 1.3: Exchanging Data

1.3.1 Compression Encryption and Hashing

Asymmetric Encryption: An encryption technique where a public key available to everyone is used to encrypt the data, and the data is decrypted by the paired private key known only by the recipient.

Dictionary Coding: A type of lossless compression where text is searched for entries that match the entries in a dictionary. Entries are substituted by a unique code which can then be translated.

Hashing: A one-way transformation of data into an abbreviated form called a hash value. The hash value is used to validate login credentials like passwords or PINs without revealing the original data to hackers.

Lossless Compression: A compression algorithm that retains all the data in the file by only storing the instructions needed to reconstruct the original file. No data is lost.

Lossy Compression: A compression algorithm that removes non-essential data from a file leading to a noticeable decrease in accuracy of the data. Data lost is non-recoverable.

Ren-Length Encoding: A type of lossless compression where repeated occurrences of the same data (like several pixels of the same colour in an image) are stored as single data values with their counts.

Symmetric Encryption: An encryption technique where the same key is used to encrypt and decrypt data. A copy of the key must be transferred between both parties.

1.3.2 Databases

Atomicity: All transactions should either succeed or fail, and never only partially processed.

Consistency: Each transaction must obey the defined validation rules of the database to maintain referential integrity.

Durability: Once a transaction has begun, it must be completed under all circumstances.

Entity-Relationship Modelling: A method of abstractly describing the data tables and the relationships between them visually. They can be used to reduce redundancy and construct a relational database.

First Normal Form (1NF): A table with no repeating attributes. The intersection of each record and attribute produces exactly one value.

Flat File Database: A database where a single table data structure is used to store all the data.

Foreign Key: A linking attribute that joins two tables in a relational database by being a primary key in one and a foreign key in the other.

Indexing: The process of creating an index of primary keys such that the location of any record can be retrieved given its primary key.

Isolation: No transaction should overwrite other transactions that are simultaneously occurring. The same results must be obtained if transactions are concurrently or sequentially processed.

Normalisation: The formal process of optimally designing data tables by reducing data redundancy and repetition by converting them into normal forms.

Primary Key: A unique identifier that identifies each record in a table.

Record Locking: A technique used to prevent simultaneous access to data in a database by locking a record when it is being edited or updated. Otherwise, inconsistencies may aries in the database

Redundancy: The unnecessary repetition of a field in multiple tables. Databases should have redundancy in the form of identical copies if part of the database gets lost and needs to be recovered.

Referential Integrity: The idea of keeping a database consistent by ensuring that any changes made to data or relationships associated with a table are accounted for in all the linked tables.

Relational Databases: A database where separate tables are made for each entity, and relationships between entities are represented by foreign keys.

Secondary Key: A key that can be used as an alternative index to access or sort records in the table in a quicker, but less accurate way than the primary key.

Second Normal Form (2NF): A table in 1NF that has data that repeats across multiple records removed and put into a new table with appropriate relationships (no partial dependencies).

Third Normal Form (3NF): A table in 2NF where all attributes that are not the primary key are fully dependent on the primary key (no non-key dependencies).

Transaction Processing: The idea of making sure that any logical operation or change in

state of a database (transaction) conforms to ACID(Atomicity, Consistency, Isolation, Durability) rules for reliable processing.

1.3.3 Networks

Circuit Switching: A method for sending data between two nodes on a network by creating a dedicated communication channel first. All data follow this same path for the duration of communication.

Client-Server Network: A type of network organisation where networked computers (clients) connect to one or more powerful central computers (servers) that handles service requests and has resources.

Domain Name System (DNS): A hierarchical naming system that maps human-readable domain names to IP addresses that locate and identify resources on a network.

Encryption: The process of converting the original data (plaintext) into a form which cannot be understood by unauthorised users (ciphertext), using an encryption algorithm (cipher).

Firewalls: A security checkpoint application that monitors incoming and outgoing network traffic, designed to prevent external users from gaining unauthorised access between two networks.

Local Area Networks (LANs): A network connecting a group of computing devices on a single geographical area/site.

Packet Switching: A method for sending data over a network by breaking data into several data packets which are sent independently and then reassembled once they all reach their destination.

Peer-to-Peer Network: A type of network organisation where networked computers are connected to each other and share resources and workloads without any central server.

Protocol Layering: A technique that simplifies network design by dividing a complex system into its component functional layers and assigning protocols for each layer to perform tasks and communicate with adjacent layers.

Proxies: A server application that intercepts all data packets entering and leaving a network to hide the true network addresses of the source from the recipient. They also restrict authorised users' access to data and isolates the network from external networks (like the internet).

Transmission Control Protocol / Internet Protocol (TCP/IP) Stack: A suite of networking protocols that allow networked computers to communicate, consisting of 4 connected layers. Incoming and outgoing data packets are passed through these layers.

Wide Area Networks (WANs): A network connecting a group of computing devices over a

large geographical area, typically with the help of third party carriers.

1.3.4 Web Technologies

Cascading Style Sheets (CSS): A style language used to define the layout, design and presentation of a webpage written in a markup language.

Client-Side Processing: The data processing and operations performed by the client. The client's browser runs the processing using the user's local computer resources. Typically used to run less critical code.

HyperText Markup Language (HTML): A markup language used to write the contents of webpages on the World Wide Web.

JavaScript: An interpreted, object-oriented programming language used to create interactive elements within web browsers for adding functionality to dynamic web pages.

PageRank Algorithm: An algorithm developed by Google to rank websites in their search results by their usefulness. It ranks a webpage's quality and importance by counting the number of links to that webpage.

Search Engine Indexing: A method of collecting, parsing and storing data from websites to facilitate fast and accurate information retrieval by the search engine. The search engineer relies on an index of webpages to accomplish this.

Server-Side Processing: The data processing and operations performed by the web server. Data is sent from the client's browser to the web server for secure processing, and the output is sent back to the client.